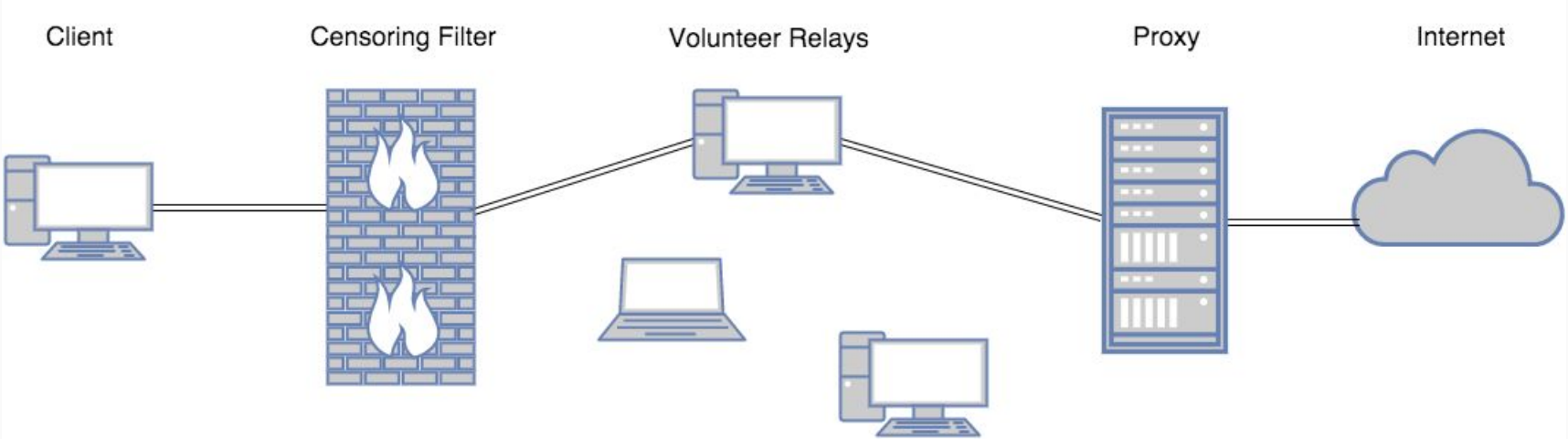
Internet Censorship Circumvention Network
::Volunteer Relay Module

Edgar Cobos

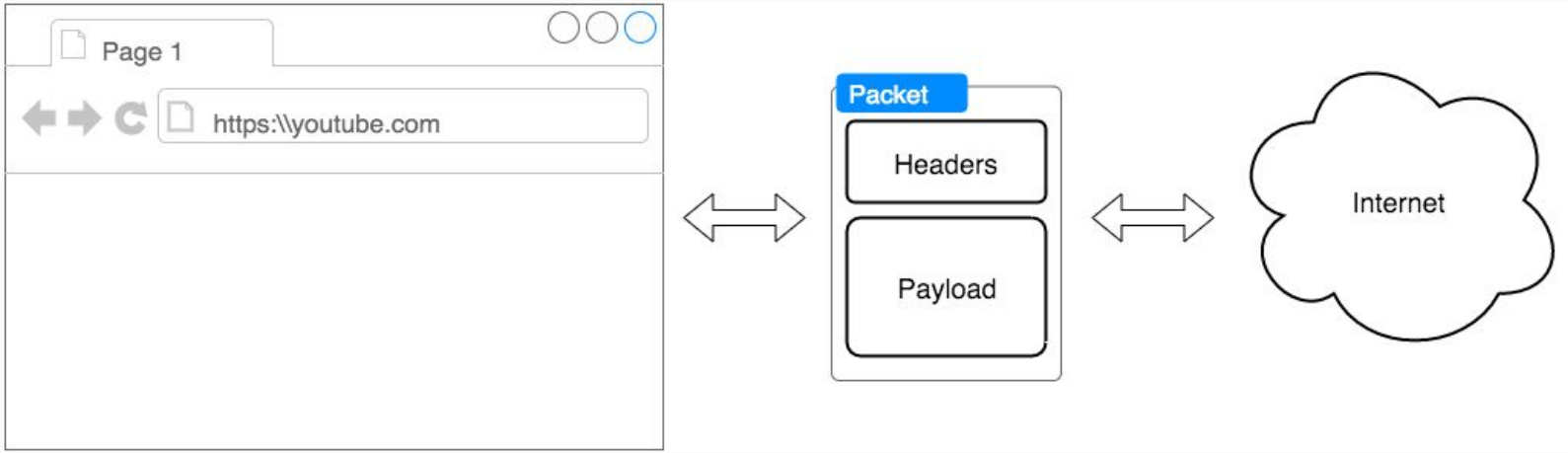
Some Background

The Bigger System

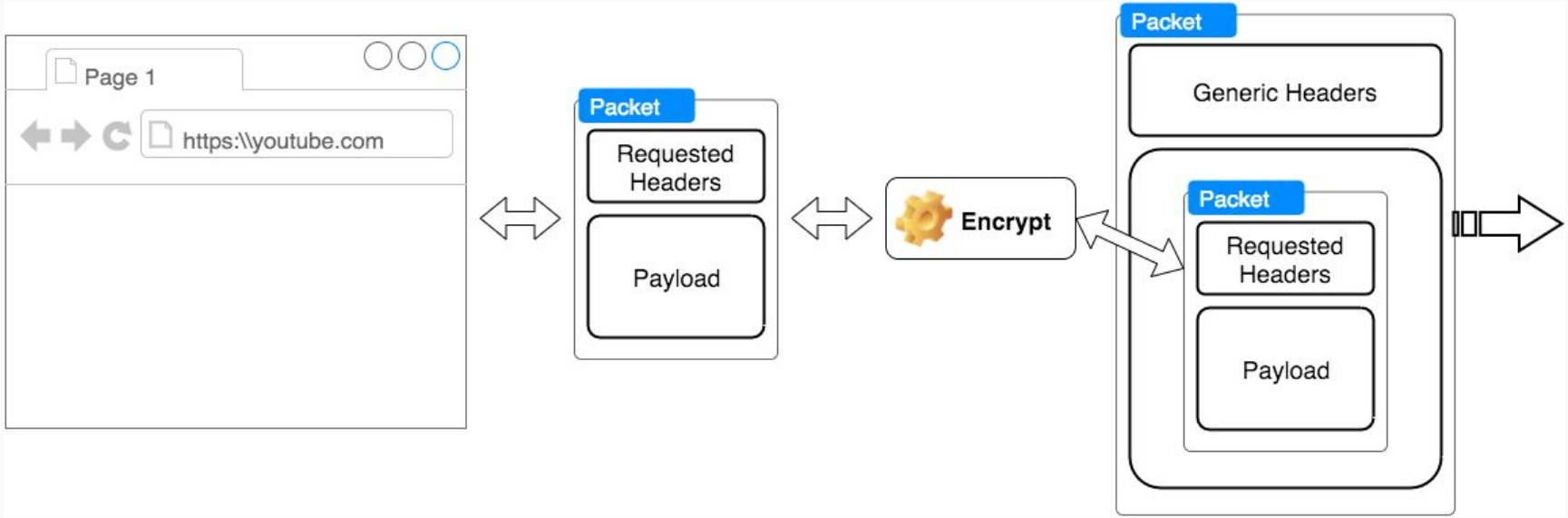
The Bigger Picture



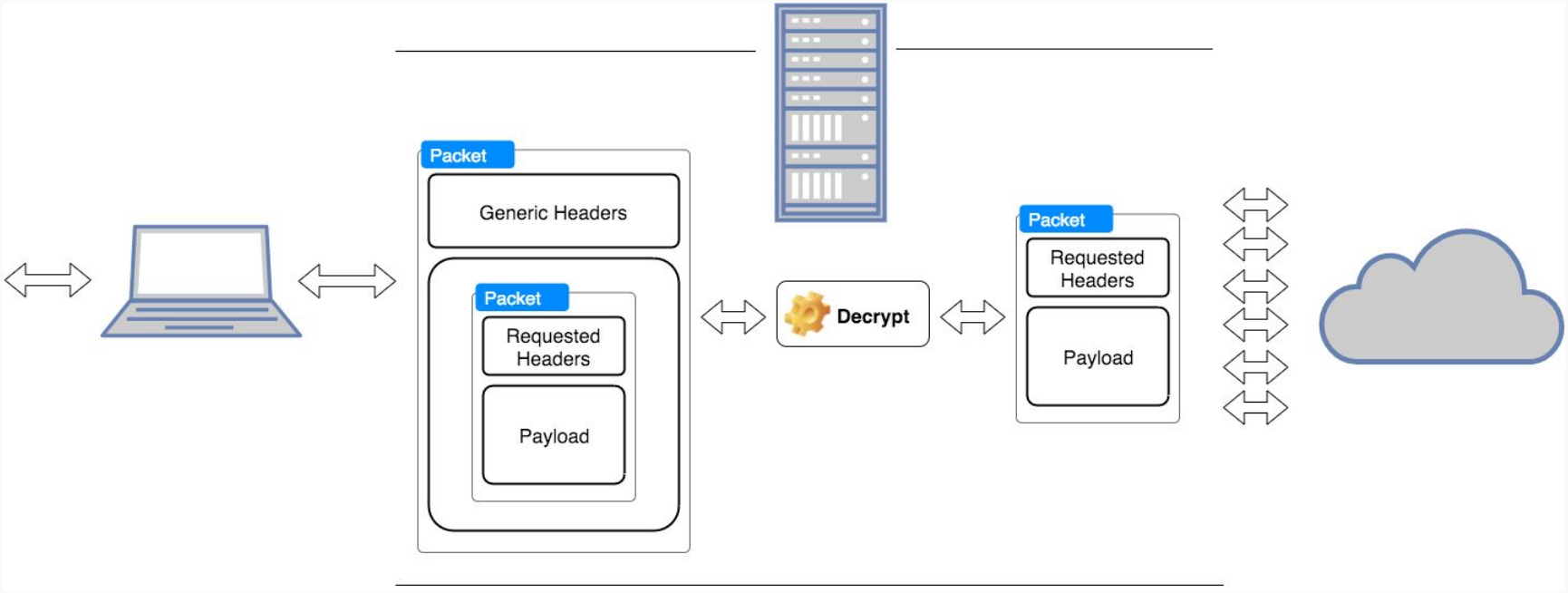
General Packet Transfer Flow



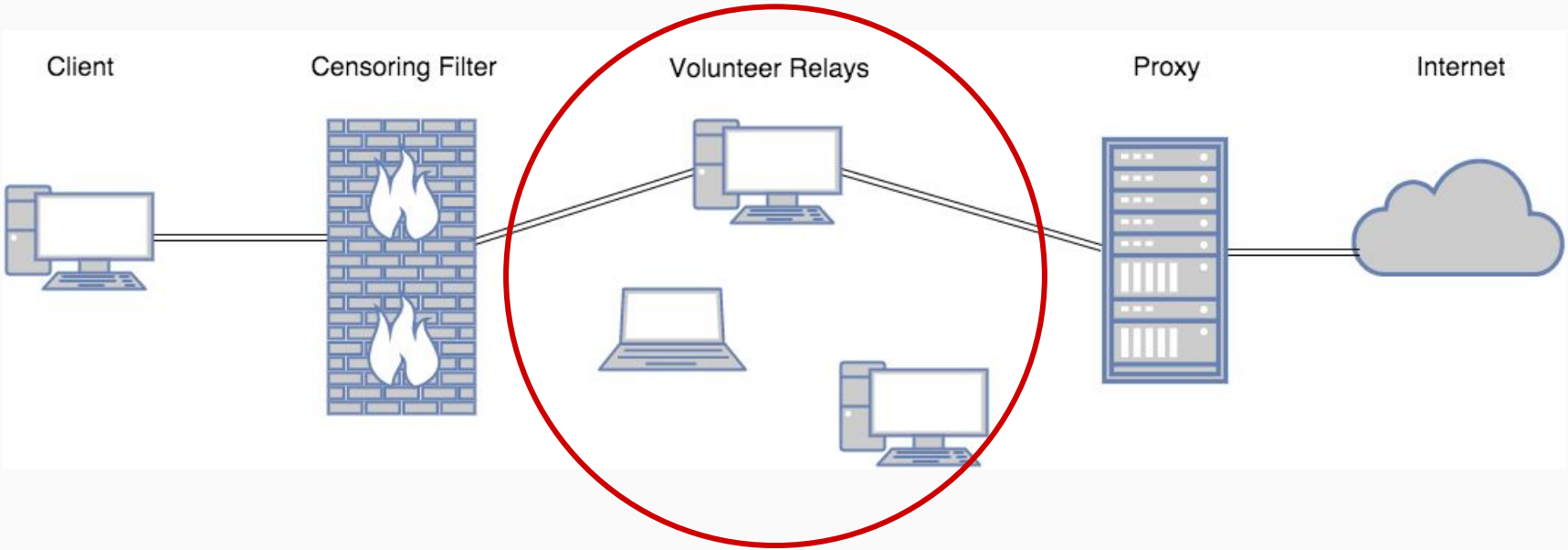
Hide Data Within Data



Relay and Fulfil the Request



The Focus

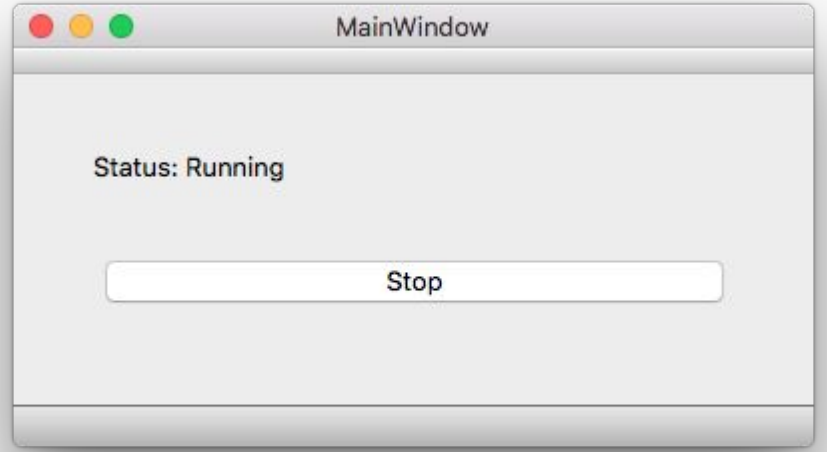


Volunteer Relay Module

Technology Used

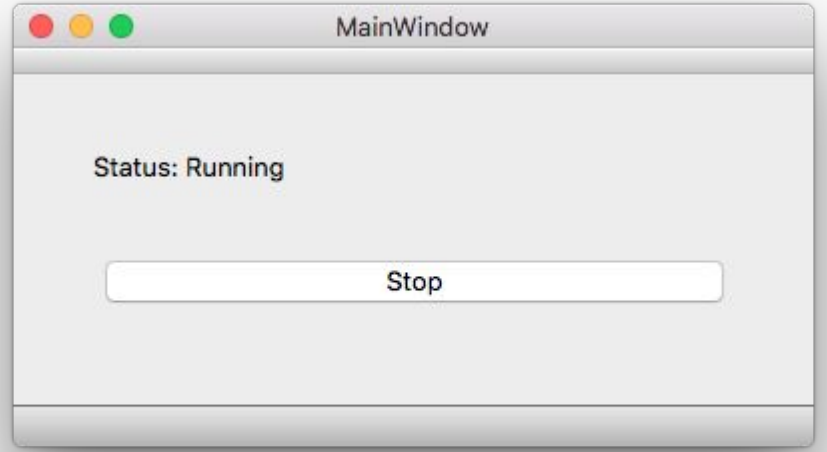
- Written in C++
- Qt Framework 5.5
- Cross-Platform
- Uses Baked-In OpenSSL 0.9.8
- Slot & Signals

I’m a Server



- Link Encryption
- TLSv1 Protocol Only
- Custom SSL Server from QTcpServer Class
- Listen For Incoming
- QSslSockets

I’m a Client



- Link Encryption
- TLSv1 Protocol Only
- Wait for Encrypted Socket Connection
- QSslSockets
- Certificate Pinning

The Tunnel

- Incoming data packets to socket buffer trigger a *Signal*
- *Slots* handle by writing bytes to the other socket buffer
- RSA/AES
- Pseudo-Random Symmetric Session Key Exchanged
- End-to-End Encryption

Future Work

- Stabilize connections
- Test on a bigger scale
- GUI
  - Display amount of bytes being transferred
  - Allow user to throttle
  - Application tampering protection

Questions?